PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-063681
(43)Date of publication of application : 12.03.1993

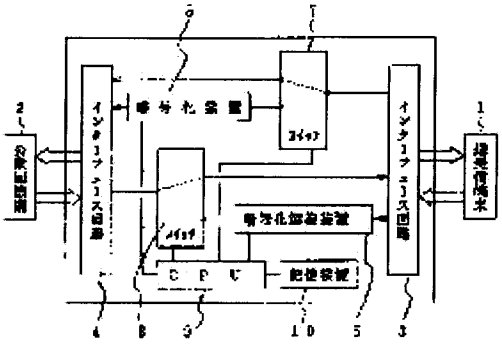
(51)Int.Cl. H04K 1/04

(21)Application number : 03-252999
(22)Date of filing : 03.09.1991

(71)Applicant : KAJIMA CORP
(72)Inventor : MURATA KIICHI
TAKAHASHI KANJIROU

(54) DEVICE FOR PREVENTING LEAKAGE OF SECRECY IN INFORMATION TRANSMISSION

(57)Abstract:
PURPOSE: To prevent leakage of secrecy for extra insurance by eliminating a care about leakage of secrecy due to mis-operation such as a specific button switch left undepressed.
CONSTITUTION: In a secrecy leakage prevention device in which a ciphering device 5 is provided to a route of a sender side when viewing from a transmission reception terminal equipment 1 as a device connecting the transmission reception terminal equipment and a line network and a ciphering decoder 6 is provided to a route of a receiver side, the input side of the ciphering device 5 is provided with a switching means 7 which is normally thrown to the position of the ciphering device and which is selected to bypass the ciphering device 5 through the release of connection to the ciphering device 5 by a specific operation, and the input side of the ciphering decoder 6 is provided with a switching means 8 which is thrown to the position of the ciphering decoder 6 when the information given to the input of the ciphering decoder 6 is ciphered and which is selected to bypass the ciphering decoder 6 when the information is not ciphered.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－63681

(43)公開日　平成5年(1993)3月12日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｋ　1/04		7117－5K		

審査請求　未請求　請求項の数1(全　5　頁)

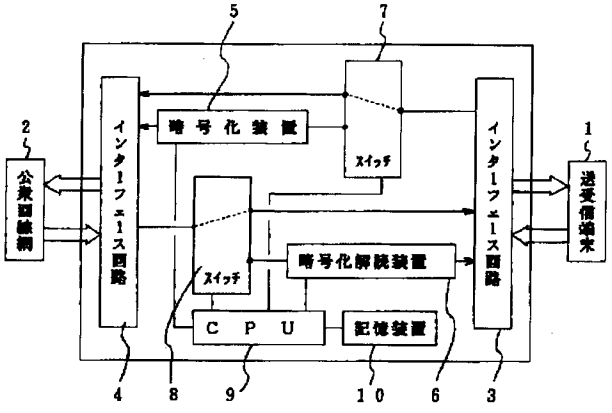
(21)出願番号　特願平3－252999

(22)出願日　平成3年(1991)9月3日

(71)出願人　000001373
鹿島建設株式会社
東京都港区元赤坂1丁目2番7号
(72)発明者　村田　喜一
東京都港区元赤坂一丁目2番7号　鹿島建設株式会社内
(72)発明者　高橋　尭爾郎
東京都港区元赤坂一丁目2番7号　鹿島建設株式会社内
(74)代理人　弁理士　久保　司

(54)【発明の名称】　情報伝送の機密漏洩防止装置

(57)【要約】
【目的】　特定ボタンスイッチの押し忘れ等の操作ミスによる機密漏洩の心配をなくし、機密漏洩防止の万全を期することができる。
【構成】　送受信端末と回線網とを接続する装置として、送受信端末１からみて送信側のルートには暗号化装置５を設け、受信側のルートには暗号化解読装置６を設ける機密漏洩防止装置において、この暗号化装置５の入力側に常時は暗号化装置５へ接続し、特定操作でこの暗号化装置５への接続を解除して暗号化装置５をバイパスさせるように切り換える切換手段７を設け、また、暗号化解読装置６の入力側に受ける情報が暗号化されている場合には暗号化解読装置６に接続し、暗号化されていない場合には暗号化解読装置６をバイパスさせるように切り換える切換手段８を設けた。



1

【特許請求の範囲】

【請求項１】　送受信端末と回線網とを接続する装置として、送受信端末からみて送信側のルートには暗号化装置を設け、受信側のルートには暗号化解読装置を設ける機密漏洩防止装置において、この暗号化装置の入力側に常時は暗号化装置へ接続し、特定操作でこの暗号化装置への接続を解除して暗号化装置をバイパスさせるように切り換える切換手段を設け、また、暗号化解読装置の入力側に受ける情報が暗号化されている場合には暗号化解読装置に接続し、暗号化されていない場合には暗号化解読装置をバイパスさせるように切り換える切換手段を設けたことを特徴とする情報伝送の機密漏洩防止装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、送受信端末から公衆回線網などの回線網を用いて情報通信を行う場合の機密漏洩防止装置に関するものである。

【０００２】

【従来の技術】現在は高度情報化社会であり、多くの重要（機密を要する）な情報が通信ネットワークを介して日常的に送受信されている。電話による会話通信やファクシミリによる伝送、コンピュータ通信などがその例である。

【０００３】このような通信ネットワークで企業内情報通信ネットワークのような専用回線を用いての通信においては、相手先が固定されているため、ＩＤコード管理、パスワード管理等のセキュリティ機能でほぼ情報もれを防ぐことができる。

【０００４】一方、公衆回線網（アナログ、デジタル）を用いて情報通信を行う場合には、ＩＤコード管理、パスワード管理だけでは充分でなく、機密漏洩・盗取に対する対策も必要となる。さらに、公衆回線網を用いる場合には操作ミスによる誤送信等についても対策をたてる必要がある。

【０００５】一例としてファクシミリで電話の公衆回線網を使用して秘密の図面や文書のの送信を行う場合に、送り先の電話番号を短縮ダイヤル等で登録しておくことで間違いのないようにすることは行われているが、短縮ダイヤルボタンの押し間違いによる誤操作は避けられない。

【０００６】近年、機密漏洩に対する対策として、元情報を各種の暗号化方式により加工し、スクランブルをかける暗号化装置と、加工された情報を前記の暗号化方式のキーによりデスクランブルをかけ、元の情報にもどす暗号化解読装置が開発されている。

【０００７】

【発明が解決しようとする課題】しかし、ＮＴＴ（日本電信電話株式会社）などで実施を試みている前記暗号化装置や暗号化解読装置を組み込む機密漏洩防止装置は、送る情報が常に暗号化されるか、もしくは特定のスイッチを押すなどの特定な操作を経て初めて暗号化されるものである。

2

【０００８】従って、送る情報が常に暗号化される場合には、受け取る側に暗号化解読装置がある受信装置がなければならず、送信先が限定されてしまう。また、特定のスイッチを押すなどの特定な操作を経て初めて暗号化されるものでは、このスイッチ操作を忘れた場合には暗号化されないで情報が送られてしまい、機密漏洩防止の役に立たない。

【０００９】本発明の目的は前記従来例の不都合を解消し、操作ミスによる機密漏洩の心配をなくし、万全を期することができる情報伝送の機密漏洩防止装置を提供することにある。

【００１０】

【課題を解決するための手段】本発明は前記目的を達成するため、送受信端末と回線網とを接続する装置として、送受信端末からみて送信側のルートには暗号化装置を設け、受信側のルートには暗号化解読装置を設ける機密漏洩防止装置において、この暗号化装置の入力側に常時は暗号化装置へ接続し、特定操作でこの暗号化装置への接続を解除して暗号化装置をバイパスさせるように切り換える切換手段を設け、また、暗号化解読装置の入力側に受ける情報が暗号化されている場合には暗号化解読装置に接続し、暗号化されていない場合には暗号化解読装置をバイパスさせるように切り換える切換手段を設けたことを要旨とするものである。

【００１１】

【作用】本発明によれば、送受信端末から送信する際に特定スイッチを押すなどの特定操作を行わない限りは切換手段が暗号化装置へ接続しており、送信された情報はこの暗号化装置でスクランブルされる。また、機密漏洩防止の必要がない情報を送信する場合は、特定スイッチを押すなどの特定操作を行うと、切換手段が切り換わり送信される情報は暗号化装置をバイパスしてそのままで送り出せる。このようにして、特定操作を忘れても暗号化が行われるので、機密は保持される。

【００１２】一方、情報を受ける側の送受信端末では、送られてくる情報が暗号化されている場合にはそのことを検知して切換手段が暗号化解読装置に接続し、デスクランブルして出力する。また、暗号化されていない場合にはそのことを検知して切換手段が切り換わり暗号化解読装置をバイパスしてそのままで出力する。

【００１３】以上の構成をとることにより、本発明の機密漏洩防止装置を備えた送受信端末同士の送受信を行う場合だけでなく、本発明の機密漏洩防止装置を備えた送受信端末とこれを備えてない送受信端末との送受信も支承なく行われ、仮に特定スイッチを押すなどの特定操作を忘れて本発明の機密漏洩防止装置を備えてない送受信端末に送信した場合には暗号化された情報が出力されるだけなので、機密漏洩のおそれはない。

【００１４】

【実施例】以下、図面について本発明の実施例を詳細に説明する。図１は本発明の情報伝送の機密漏洩防止装置のブロック図で、送受信端末１と公衆回線網２とを接続する装置として、送受信端末１側のインターフェース回路３と公衆回線網２側のインターフェース回路４との間で、送受信端末１からみて送信側のルートには暗号化装置（スクランブラー）５が設けられ、受信側のルートには暗号化解読装置（デスクランブラー）６が設けられる。

【００１５】暗号化装置５は、元情報（データ）を各種の暗号化方式により加工し、スクランブルをかけるものであり、また、暗号化解読装置６は加工された情報（データ）を前記の暗号化方式のキーによりデスクランブルをかけ、もとの情報（データ）に戻すものである。図４にこの暗号化装置５、暗号化解読装置６の構成を示すが、鍵処理部11には暗号鍵／復号鍵12からの出力が導入され、この鍵処理部11からの出力で、前処理→データかく拌処理→データかく拌処理→後処理という処理が行われる。

【００１６】インターフェース回路３，４は、ＣＣＩＴＴ（国際電信電話諮問委員会）の規格であるＶインターフェース、Ｘインターフェース、Ｉインターフェースや ＩＥＥＥ（アメリカ電気電子技術者協会）の規格であるＧＰ―ＩＢ、ＥＩＡ（米国電子工業会）の規格であるＲＳ―２３２Ｃ、ＮＴＴ（日本電信電話株式会社）の規格であるＹインターフェース等をその都度接続する網、端末により使い分けるようにすればよい。

【００１７】前記暗号化装置５の入力側に、常時は暗号化装置５へ接続し、押しボタンスッチ等の特定操作でこの暗号化装置５への接続を解除して暗号化装置５をバイパスさせるように切り換えるスイッチ等による切換手段７を設ける。

【００１８】また、暗号化解読装置６の入力側に、受ける情報が暗号化されている場合には暗号化解読装置６に接続し、暗号化されていない場合には暗号化解読装置６をバイパスさせるように切り換えるスイッチ等による切換手段８を設けた。なお、暗号化装置５、暗号化解読装置６および切換手段７，８はＣＰＵ（中央処理装置）９に接続され、さらにこのＣＰＵ９は記憶装置（メモリ）10を接続している。なお、該ＣＰＵ９には切換手段８に入力される情報が暗号化されものであるか否かを自動的に判別して切換手段８を切り換えるように指令信号を発する判別手段が形成される。この判別手段は受ける情報がデジタル信号であれば、頭の何ビットかでその判断を行うものである。

【００１９】次に、使用法について説明する。図２はファクシミリ通信の場合の送信フローを示すもので、相手先のダイヤルを回し、相手先に本発明装置が無い場合には特定スイッチとしてのスルーボタンを押してから、送信ボタンを押す。これにより、切換手段７が作用して暗号化装置５をバイパスしてそのままの状態で送信が行われる。

【００２０】相手先に本発明装置がある場合には、そのまま送信ボタンを押す。切換手段７はインターフェース回路３と暗号化装置５とを接続し、情報は暗号化装置５で暗号化されて送信される。

【００２１】図３は着信フローを示すもので、着信される情報が暗号化されている場合にはそのことを検知して切換手段が暗号化解読装置６に接続し、デスクランブル（解説）して受信する。また、暗号化されていない場合にはそのことを検知して切換手段８が切り換わり暗号化解読装置６をバイパスしてそのままで受信する。

【００２２】なお、オプション機能をして、予め通信相手先を登録設定しておき、通信毎に先ず相手先を確認してから通信を開始するようにしてもよい。この場合には相手方が登録されていない時には通信を中止する。

【００２３】

【発明の効果】以上述べたように本発明の情報伝送の機密漏洩防止装置は、特定ボタンスイッチの押し忘れ等の操作ミスによる機密漏洩の心配をなくし、機密漏洩防止の万全を期することができるものである。

【図面の簡単な説明】

【図１】本発明の情報伝送の機密漏洩防止装置の１実施例を示すブロック図である。

【図２】送信時の動作を示すフロー図である。

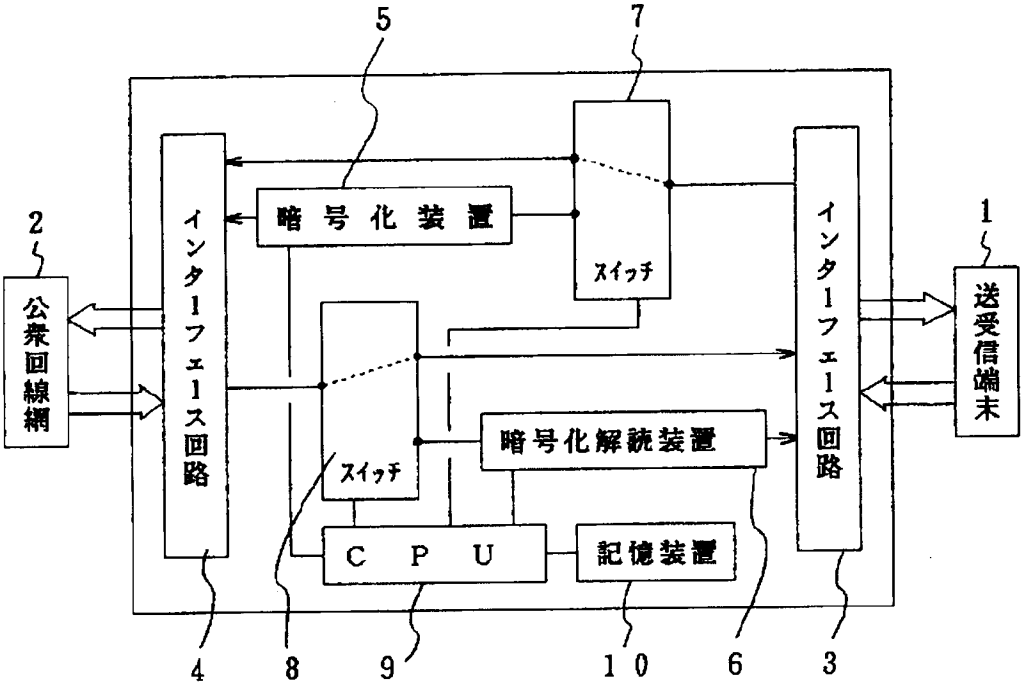
【図３】着信時の動作を示すフロー図である。

【図４】暗号化装置、暗号化解読装置の説明図である。

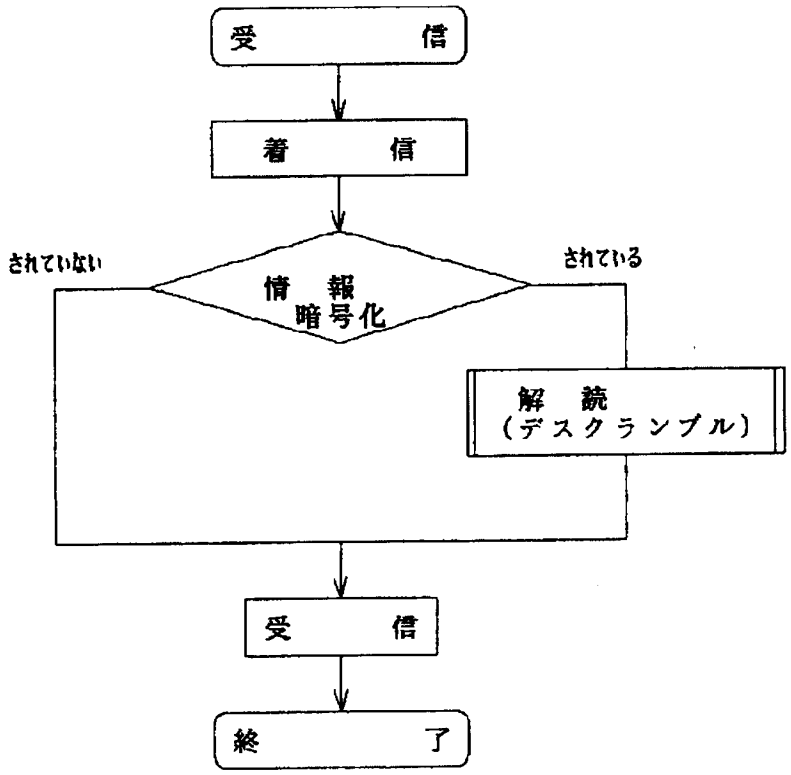
【符号の説明】

１…送受信端末	２…公衆回線網
３，４…インターフェース回路	５…暗号化装置
６…暗号化解読装置	７，８…切換手段
９…ＣＰＵ	10…記憶装置
11…鍵処理装置	12…暗号鍵／復号鍵

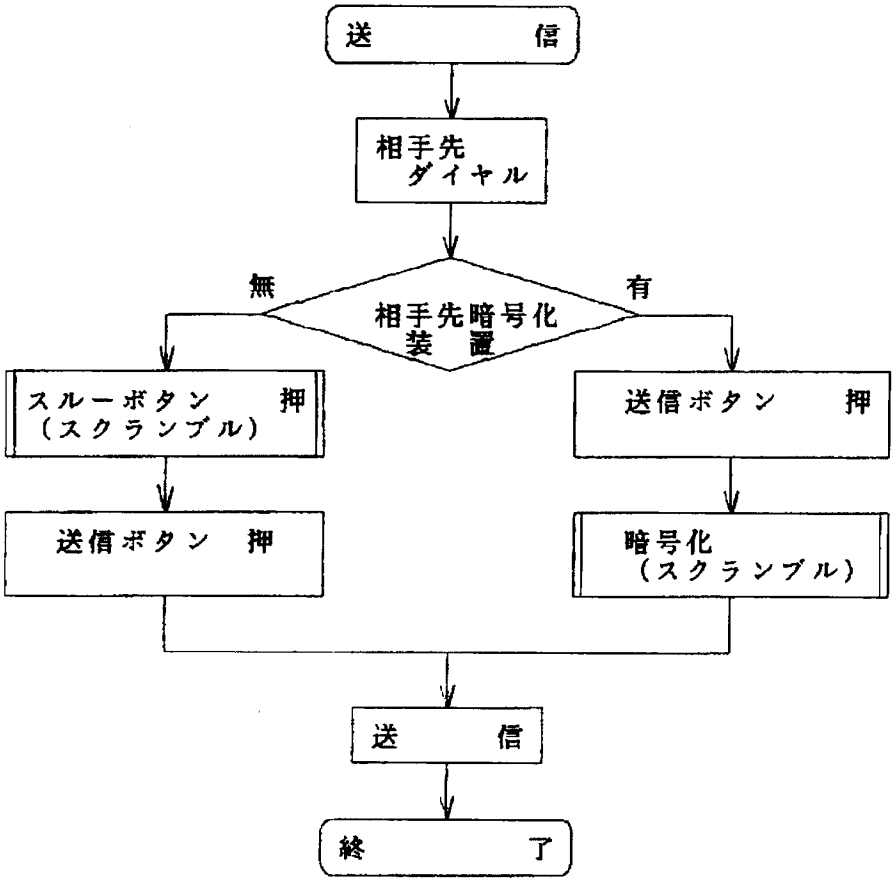
【図１】


5
7
2
1
暗号化装置
スイッチ
インターフェース回路
公衆回線網
送受信端末
暗号化解読装置
スイッチ
C P U
記憶装置
4
8
9
10
6
3

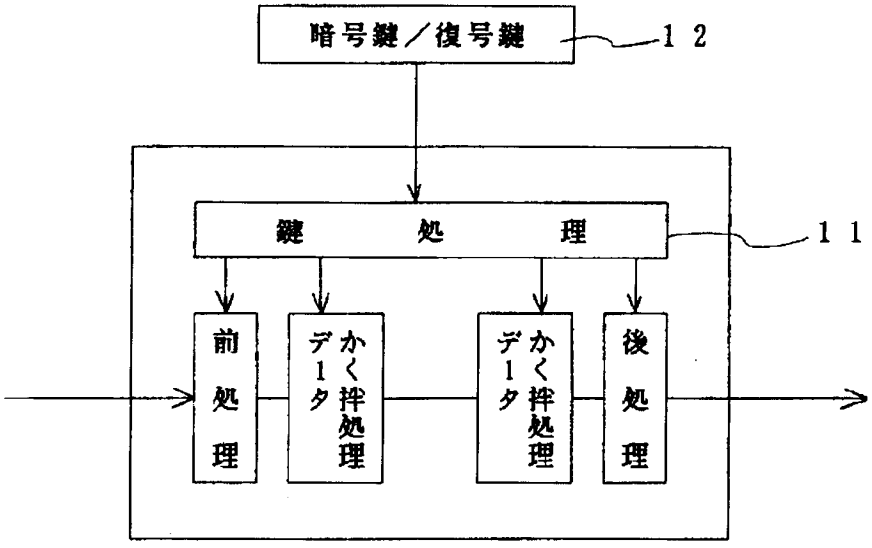
【図３】


受　信
着　信
されていない
情報暗号化
されている
解読（デスクランブル）
受　信
終　了

【図２】


送　　信
相手先
ダイヤル
無
相手先暗号化
装　置
有
スルーボタン　　押
（スクランブル）
送信ボタン　　押
送信ボタン　押
暗号化
（スクランブル）
送　　信
終　　了

【図４】


暗号鍵／復号鍵
12
鍵　処　理
11
前処理
かく拌処理データ
かく拌処理データ
後処理